Security Principles: Defenses

SPR500 NBB

Project

Security Testing Report

Group 2	
Student Name	**Student ID**
Khondoker Ishmum Muhammad	155895212
Yash Siraj Devani	160409215
Ananthu Krishna Vadakkeppatt	154290217
Aryan Santosh Saindane	136235215

Table Of Contents

Executive Summary

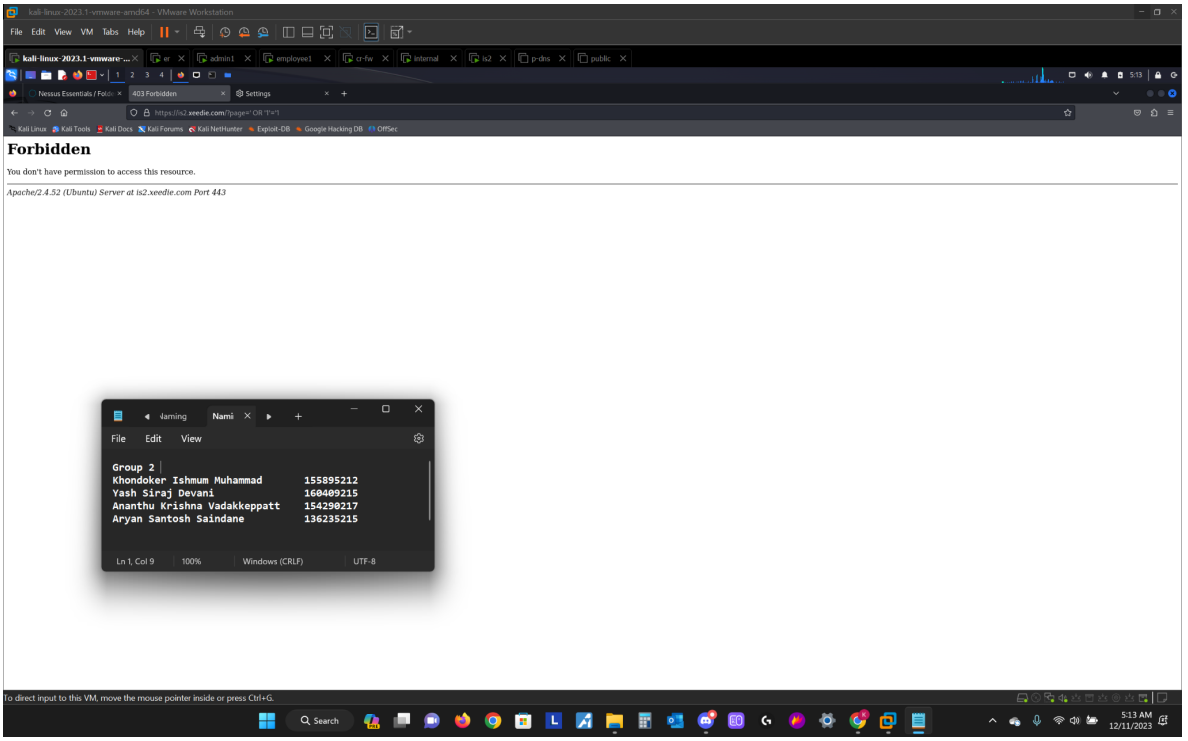
The objective of this report is to highlight the testing of security controls implemented in the Agricore infrastructure. Recognizing the pivotal role of security controls in protecting digital assets and sensitive information within the domain, the report emphasizes the proactive identification and mitigation of vulnerabilities and weaknesses. Utilizing security control testing serves as a strategic approach to fortify defenses against potential threats, ensuring the integrity of networks, and instilling confidence with clients. The security controls, implemented in accordance with the CIS framework, are central to this discussion. The report aims to elucidate the process of adding and testing these controls within the Agricore infrastructure.

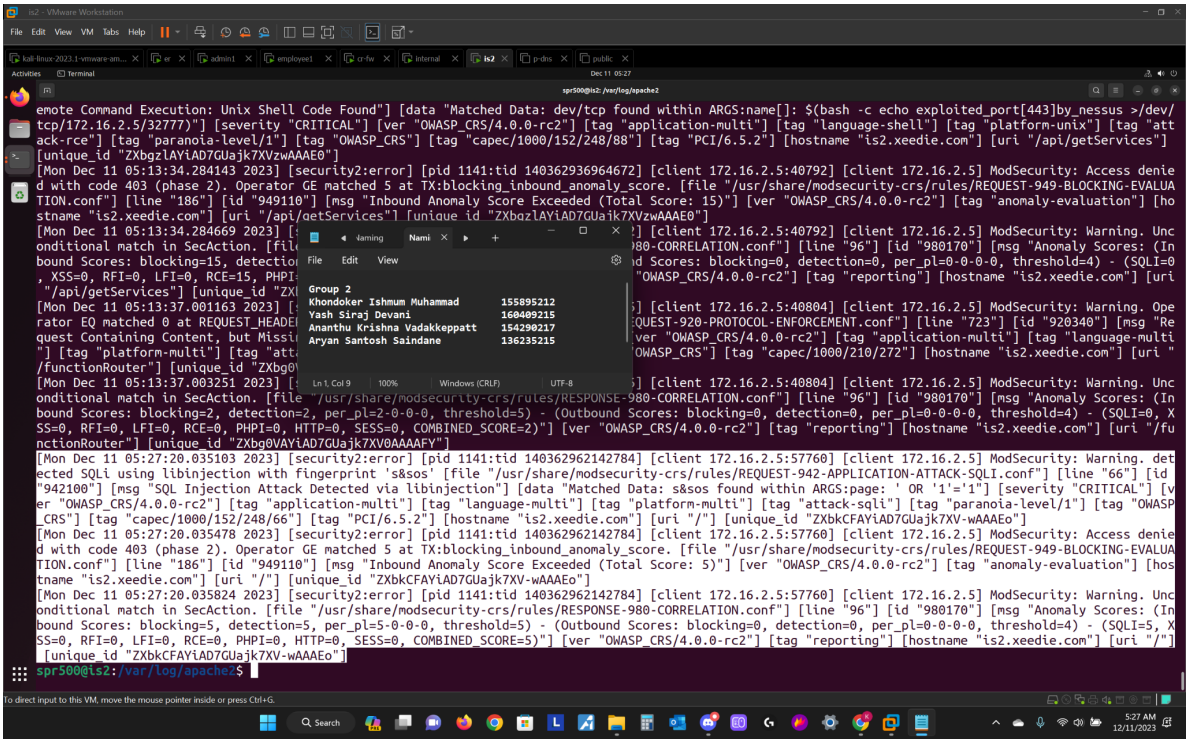
Recommended Controls & Controls Tested Based On CIS

Below we showcase 18 security controls that are based on the CIS controls. These controls will help ensure proper security posture for the organizations and allow smooth business operations.

1. SQL Injection Prevention

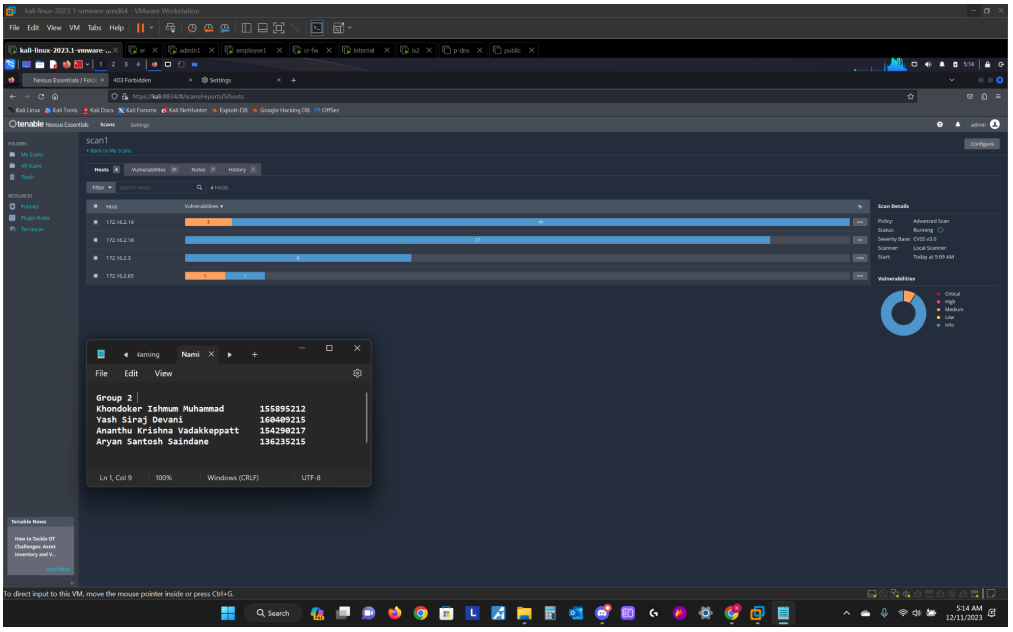
- Implementing a Web Application Firewall (WAF) is crucial for enhancing the security posture of your web applications. SQL Injection blocked and logged.





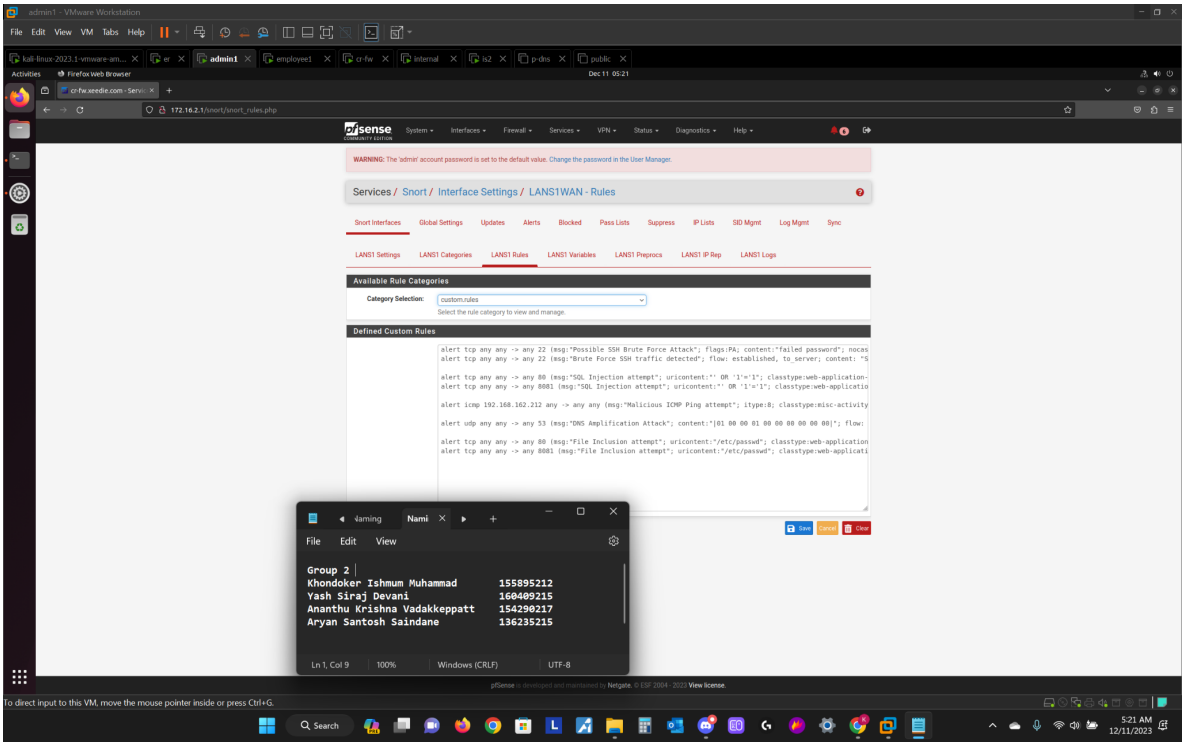
2. Vulnerability Scanning

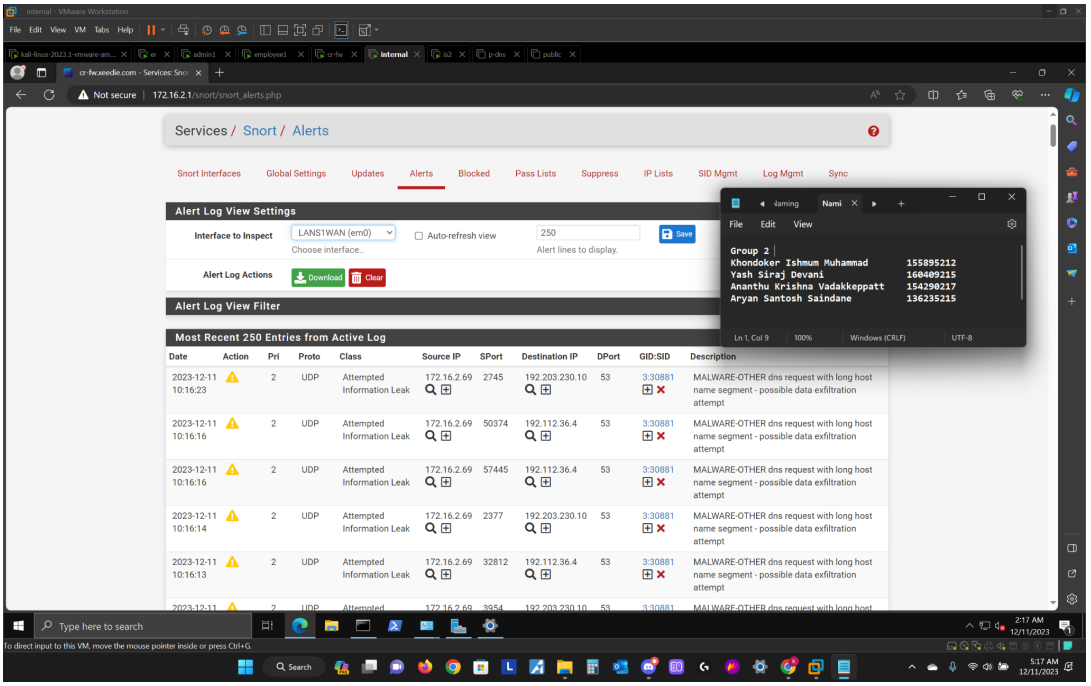
- Utilize automated vulnerability scanning tools to identify and prioritize patching for critical vulnerabilities. Utilize nessus for scanning or nmap.



3. Proactive Monitoring

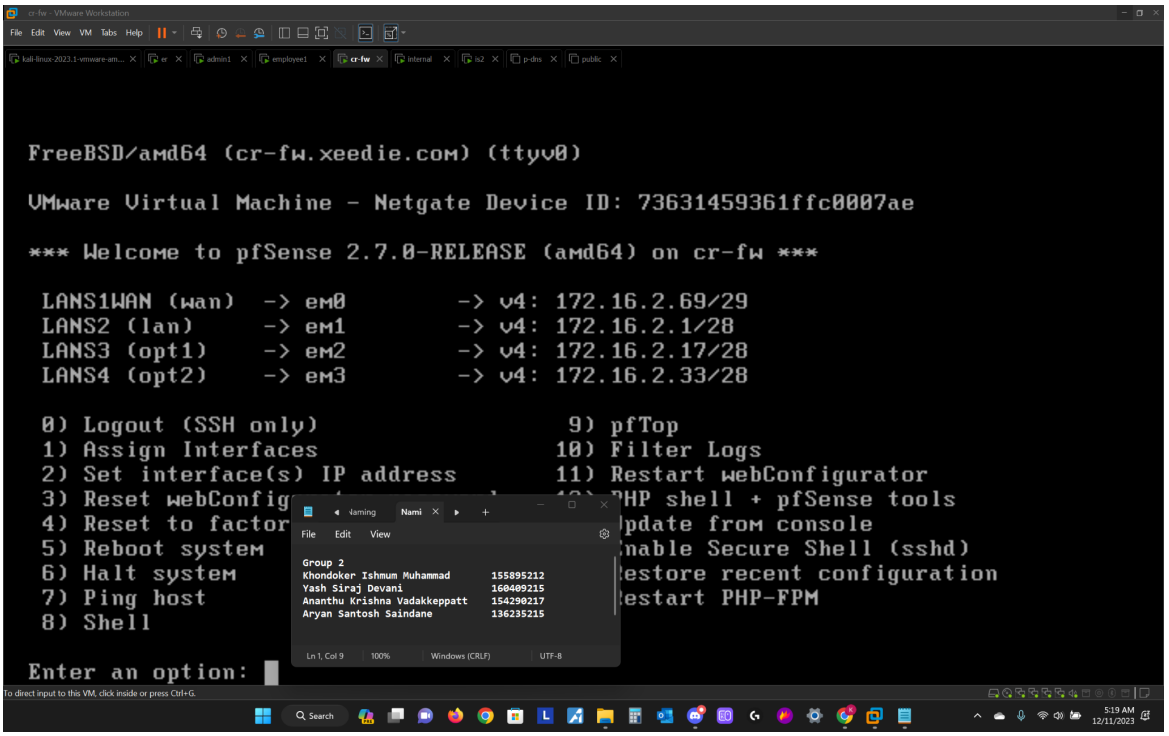
- Emphasize the importance of proactive monitoring for early detection of security incidents. Utilize Snort IDS to monitor traffic. Also utilize custom snort rules.

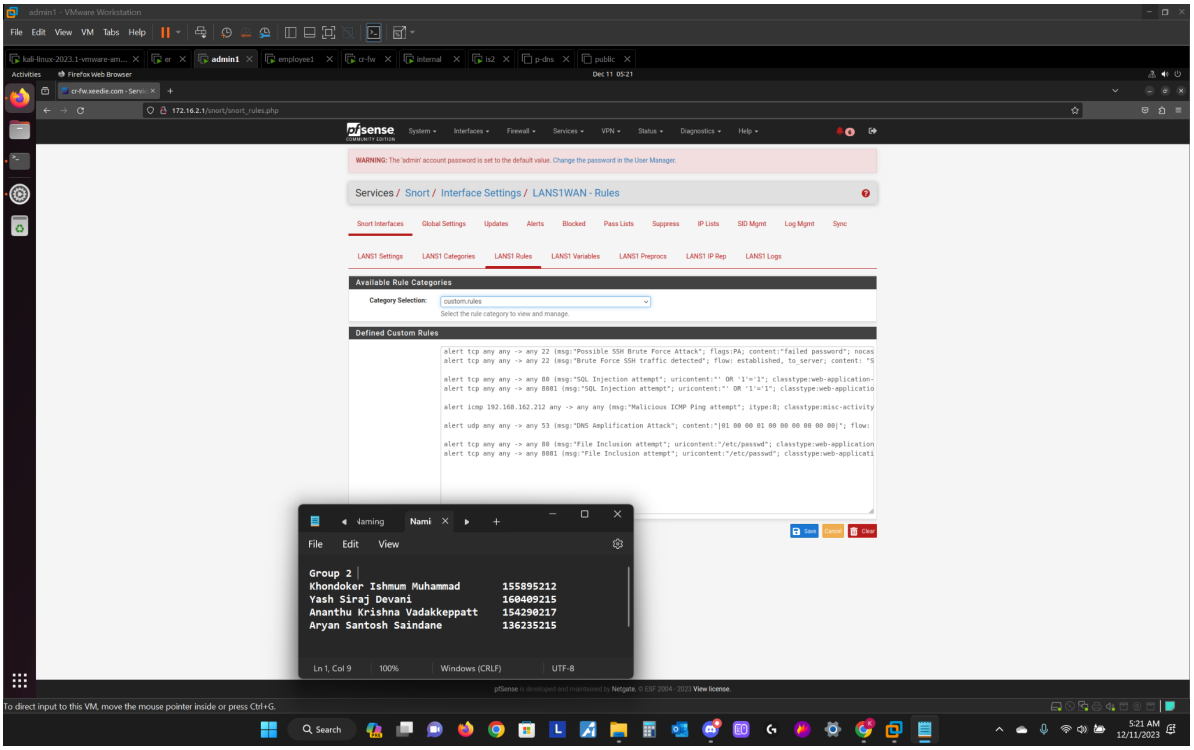




4. Network Segmentation Validation

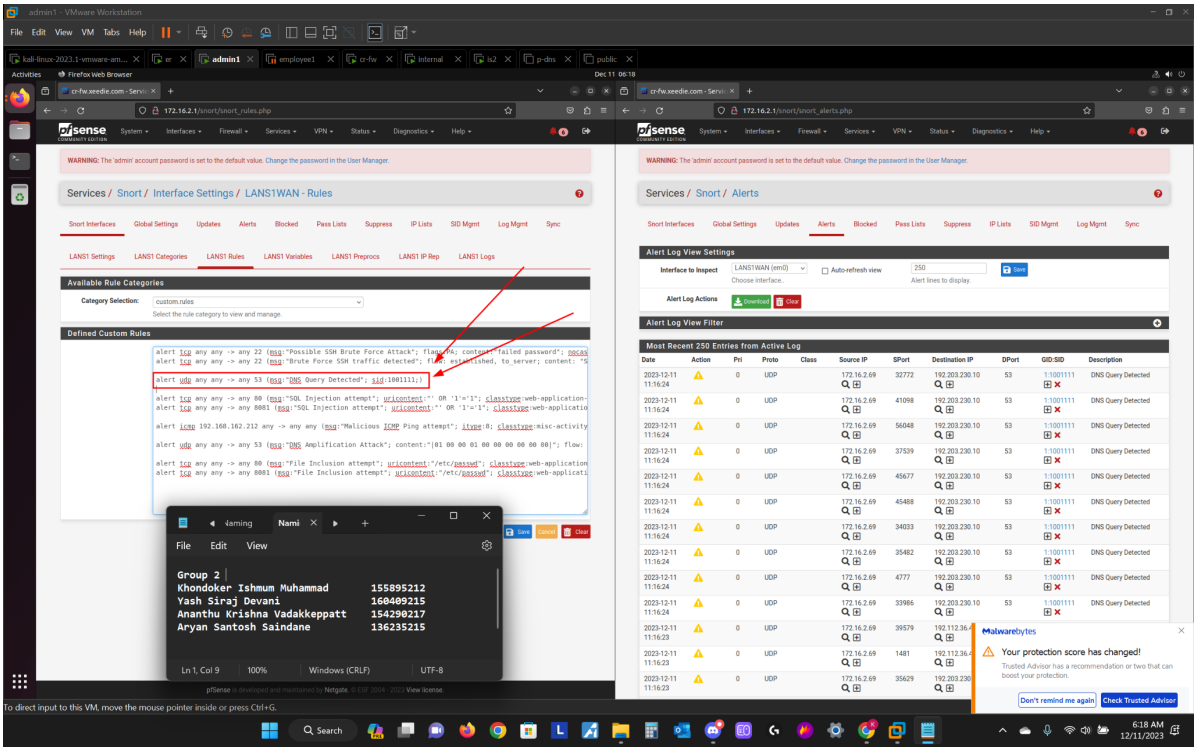
- Include a recommendation to conduct regular penetration testing to validate the effectiveness of network segmentation controls. Creating different LANs for different parts of our networks.





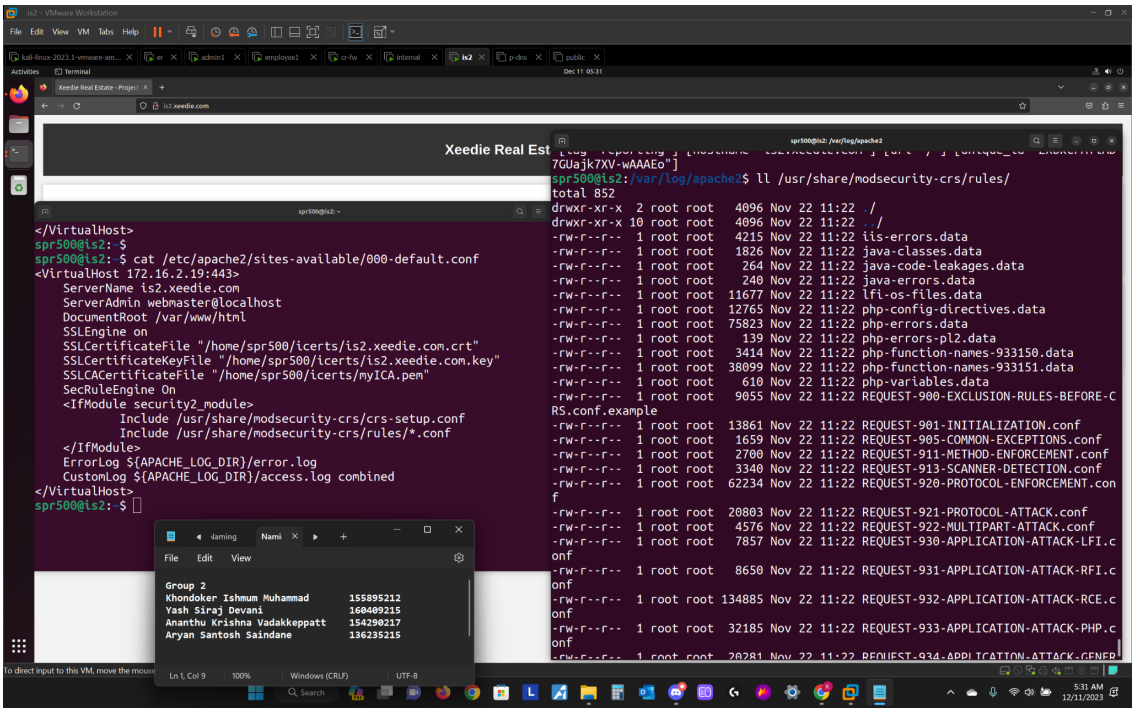
5. Continuous DNS Monitoring

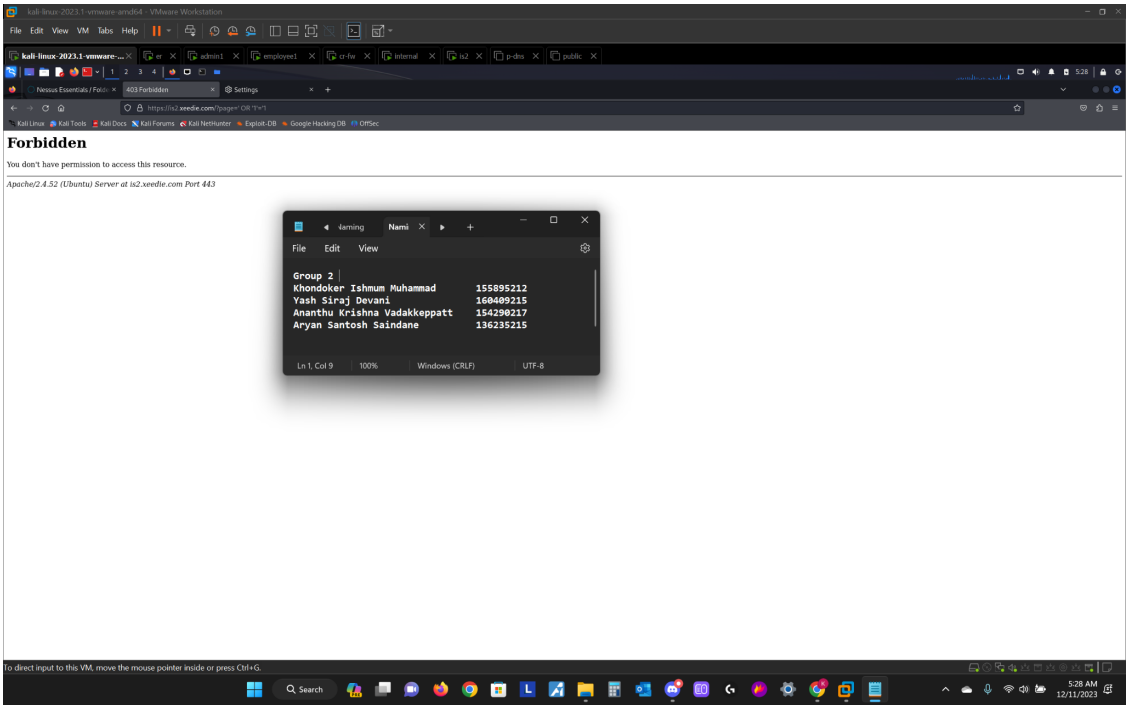
- Emphasize the importance of continuous monitoring and timely response to DNS-related security events. Snort IDS can be used here.

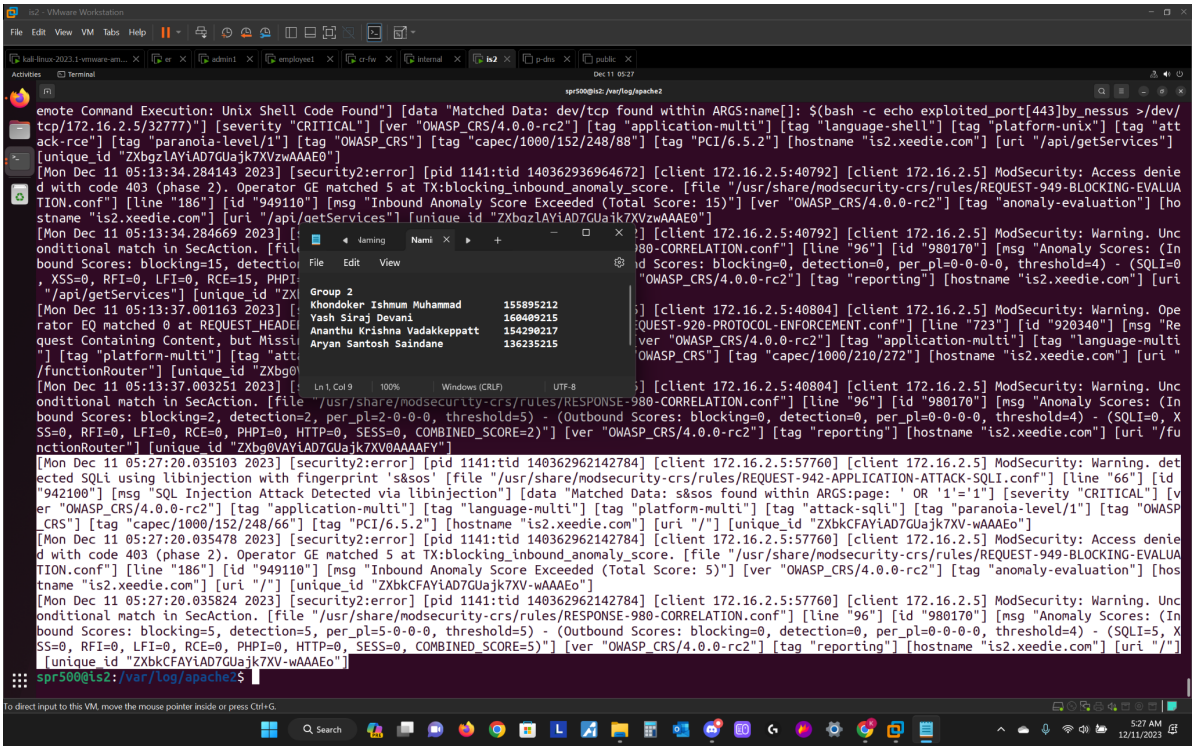


6. Web Application Security

- Implementing Web Applications Firewall (WAFs) to monitor and filter HTTP traffic, enhancing protection against input validation vulnerabilities. Utilize Mod Security. Below we can see mod security blocking and logging the sql injection attack.

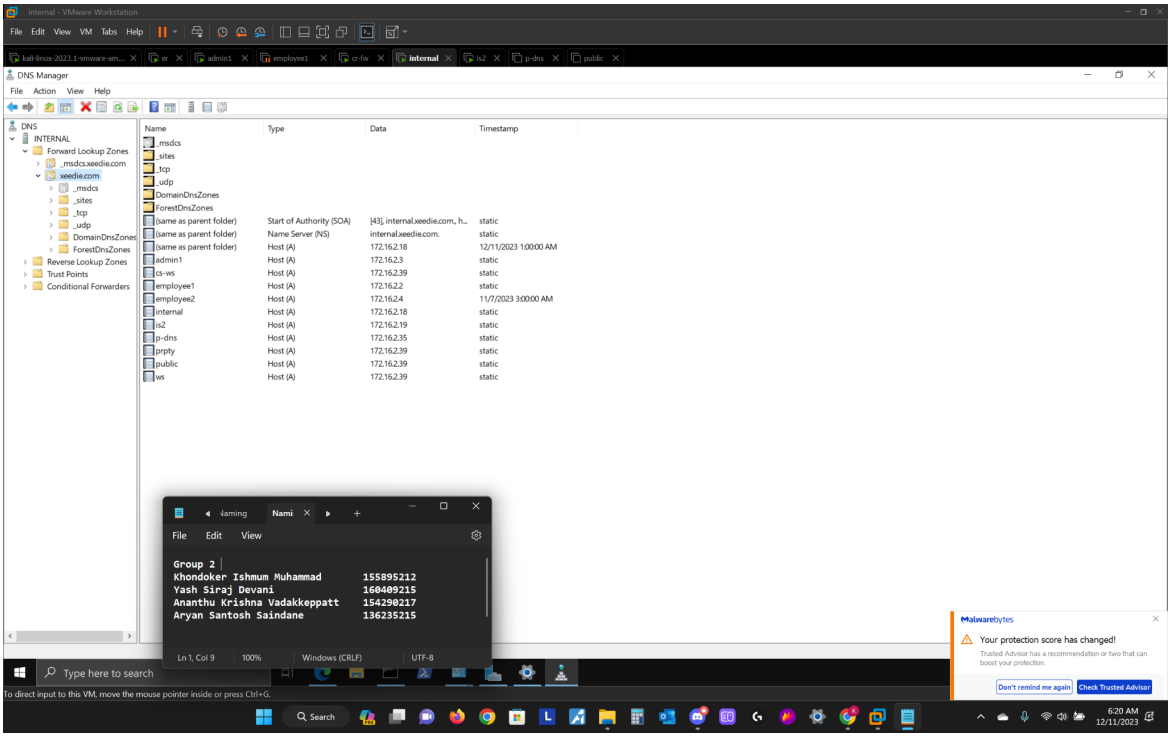






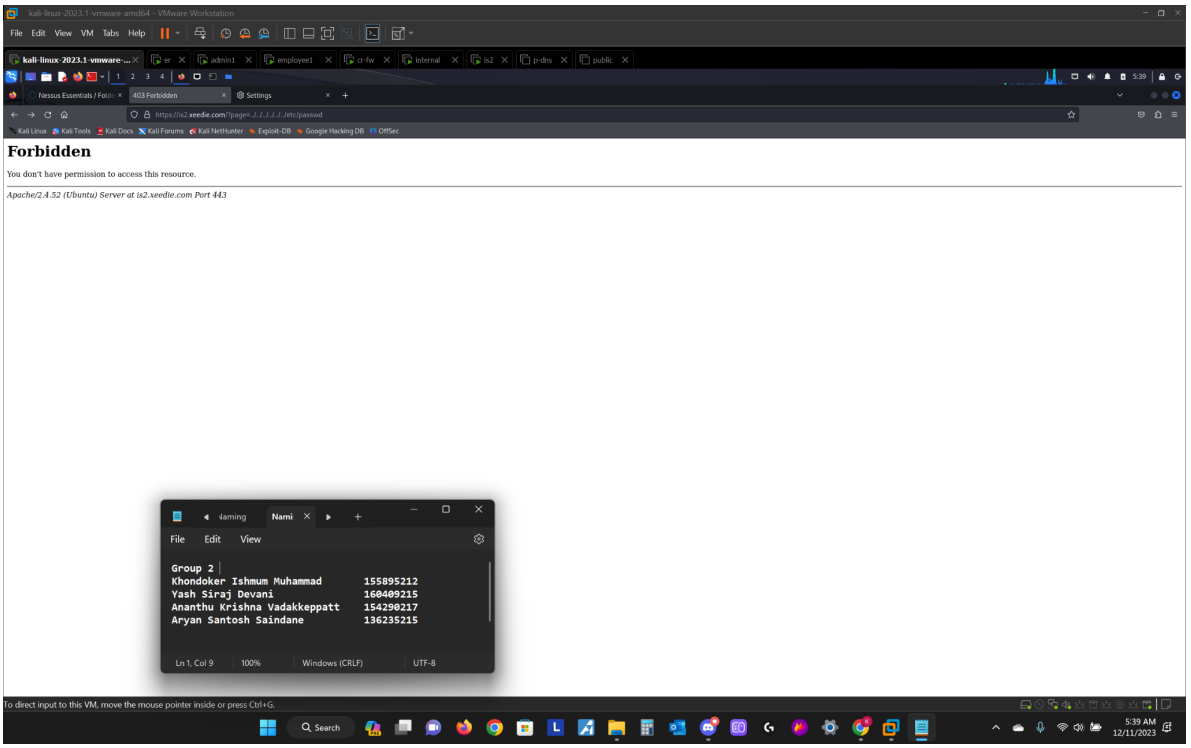
7. DNS Security

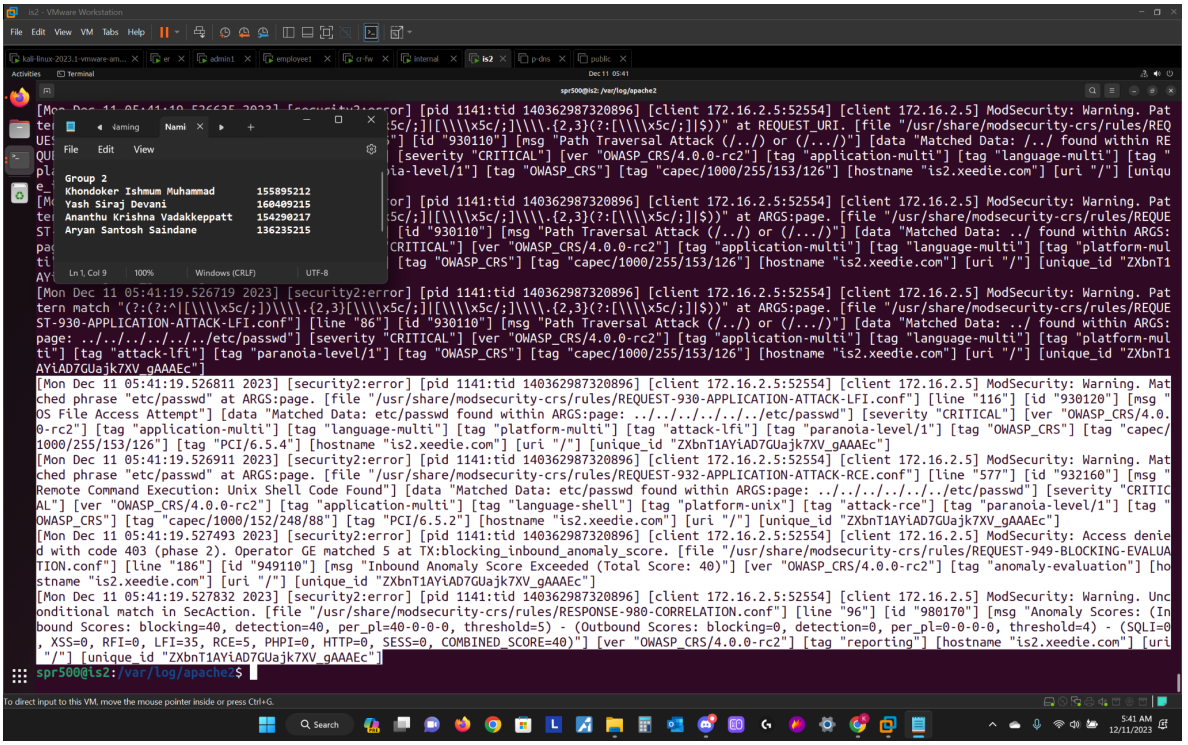
- Regularly review and update DNS configurations to ensure the integrity and security of DNS services.



8. File Inclusion Prevention

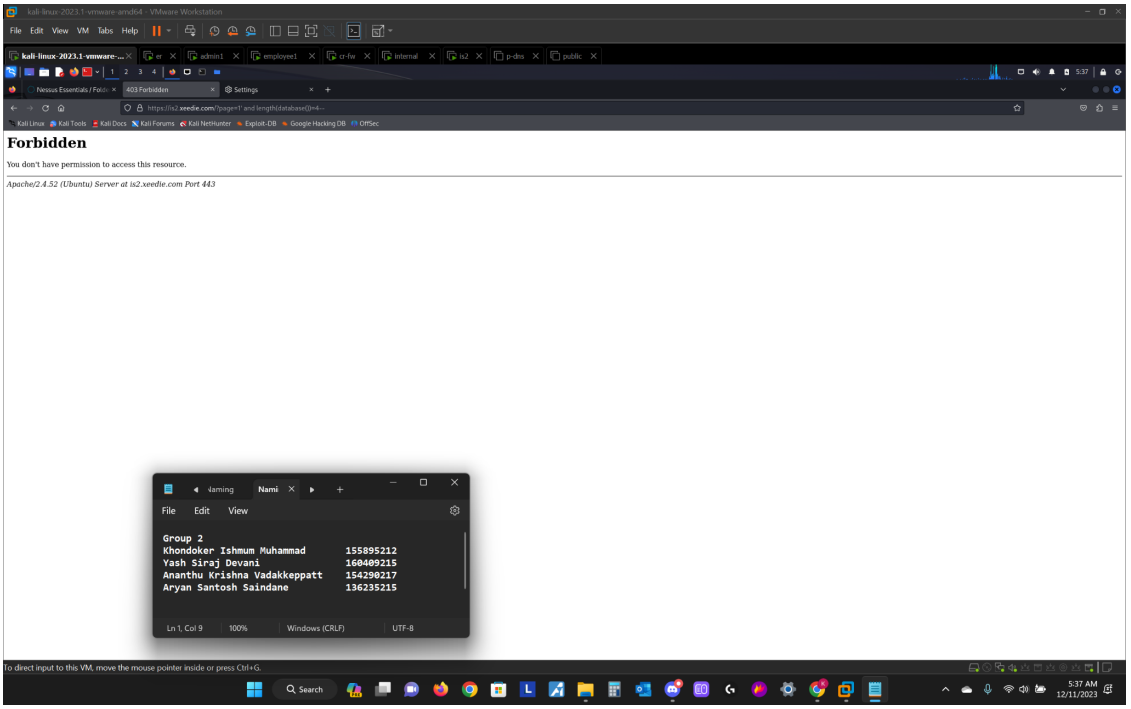
- Deploy a WAF to monitor and filter HTTP traffic, providing an additional layer of defense against file inclusion vulnerabilities. File inclusions attack blocked and logged.





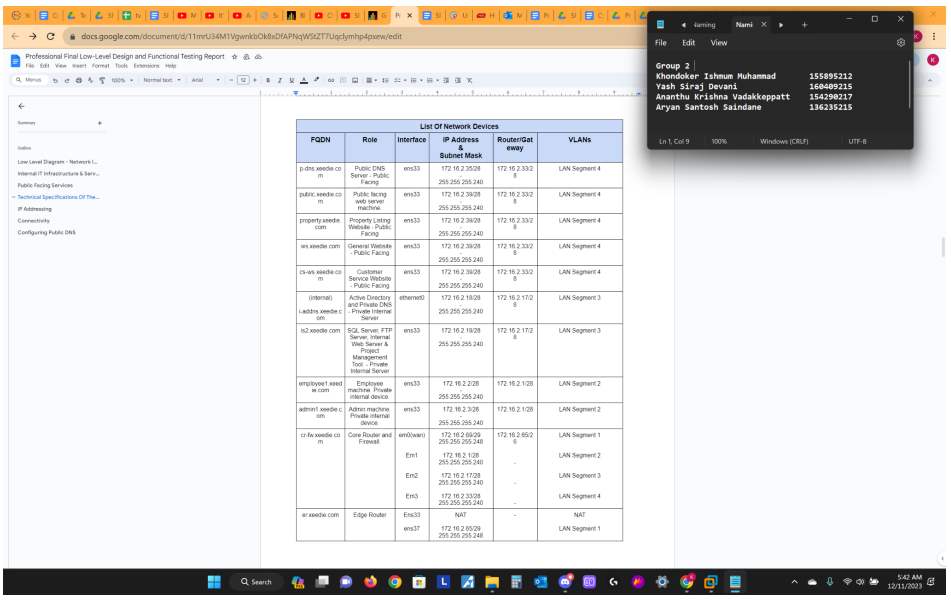
9. SQL Injection Blind

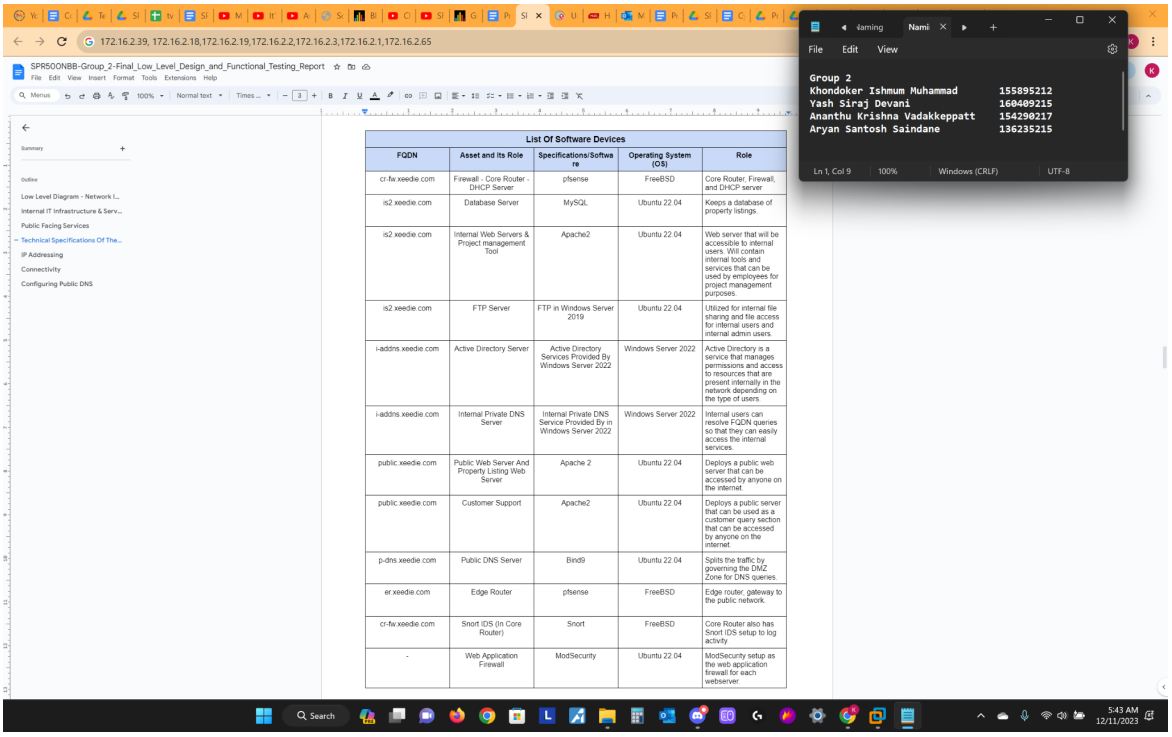
- Deploy a WAF to actively monitor and filter HTTP traffic, providing an effective defense against Blind SQL Injection attempts.



10. Company asset (hardware & software) management

- Crucial for compliance and cost optimization, involves tracking software assets, including installed applications, across the organization's end-user devices, servers, and virtual environments.





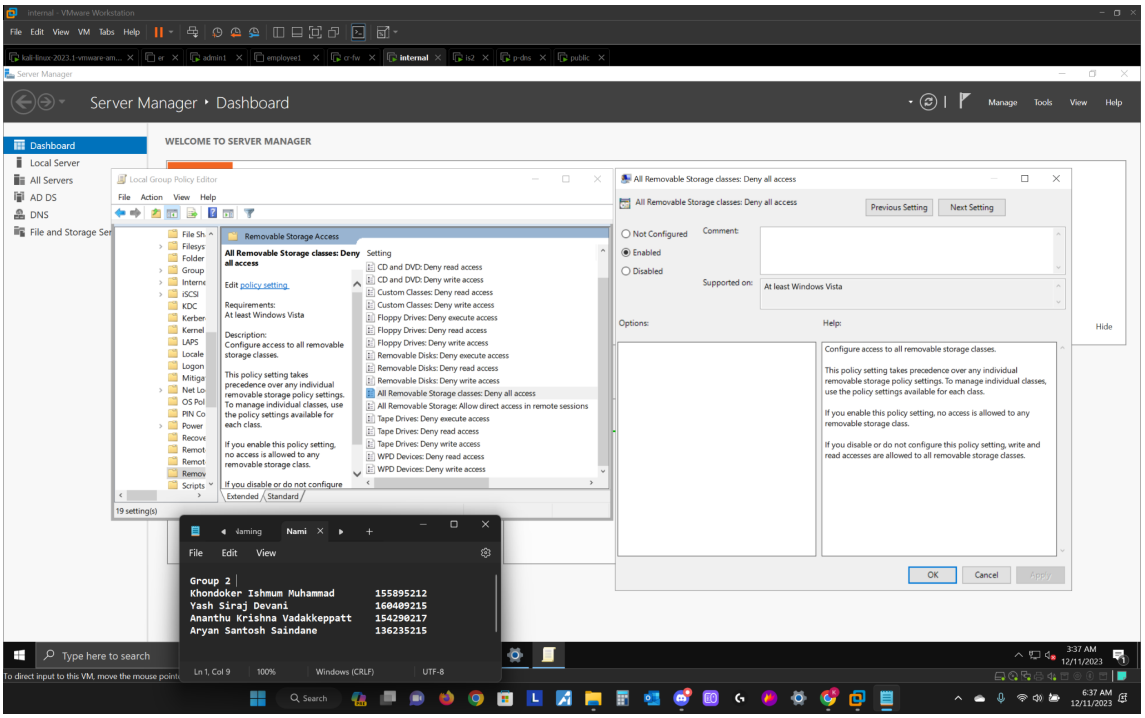
List Of Software Devices

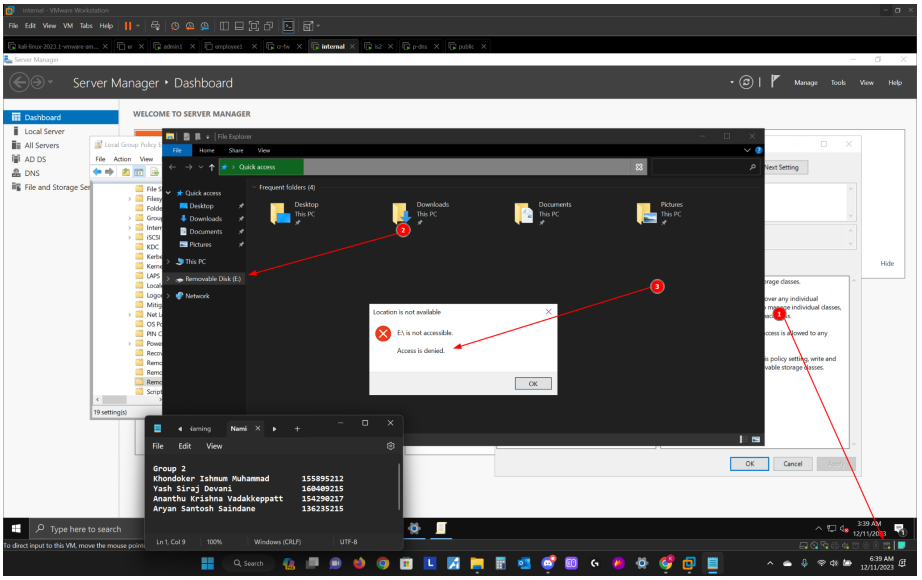
FQDN	Asset and Its Role	Specifications/Software	Operating System (OS)	Role
cr-fw.xeedie.com	Firewall - Core Router - DHCP Server	pfsense	FreeBSD	Core Router, Firewall, and DHCP server
is2.xeedie.com	Database Server	MySQL	Ubuntu 22.04	Keeps a database of property listings.
is2.xeedie.com	Internal Web Servers & Project management Tool	Apache2	Ubuntu 22.04	Web server that will be accessible to internal users. Will contain internal tools and services that can be used by employees for project management purposes.
is2.xeedie.com	FTP Server	FTP in Windows Server 2019	Ubuntu 22.04	Utilized for internal file sharing and file access for internal users and internal admin users.
i-addns.xeedie.com	Active Directory Server	Active Directory Services Provided By Windows Server 2022	Windows Server 2022	Active Directory is a service that manages permissions and access to resources that are present internally in the network depending on the type of users.
i-addns.xeedie.com	Internal Private DNS Server	Internal Private DNS Service Provided By in Windows Server 2022	Windows Server 2022	Internal users can resolve FQDN queries so that they can easily access the internal services.
public.xeedie.com	Public Web Server And Property Listing Web Server	Apache 2	Ubuntu 22.04	Deploys a public web server that can be accessed by anyone on the internet.
public.xeedie.com	Customer Support	Apache2	Ubuntu 22.04	Deploys a public server that can be used as a customer query section that can be accessed by anyone on the internet.
p-dns.xeedie.com	Public DNS Server	Bind9	Ubuntu 22.04	Splits the traffic by governing the DMZ Zone for DNS queries.
er.xeedie.com	Edge Router	pfsense	FreeBSD	Edge router, gateway to the public network.
cr-fw.xeedie.com	Snort IDS (In Core Router)	Snort	FreeBSD	Core Router also has Snort IDS setup to log activity
-	Web Application Firewall	ModSecurity	Ubuntu 22.04	ModSecurity setup as the web application firewall for each webserver.

```
Group 2
Khondoker Ishmum Muhammad      155895212
Yash Siraj Devani              160409215
Ananthu Krishna Vadakkeppatt   154290217
Aryan Santosh Saindane         136235215
```

11. Malware Defense Control

- Implementing critical malware defense measures, we disabled autorun on all connected devices through a Group Policy Object (GPO), preventing the automatic execution of malware on USB drive connection, and extended this control to Proxmox infrastructure, prohibiting the attachment of removable devices for enhanced security.



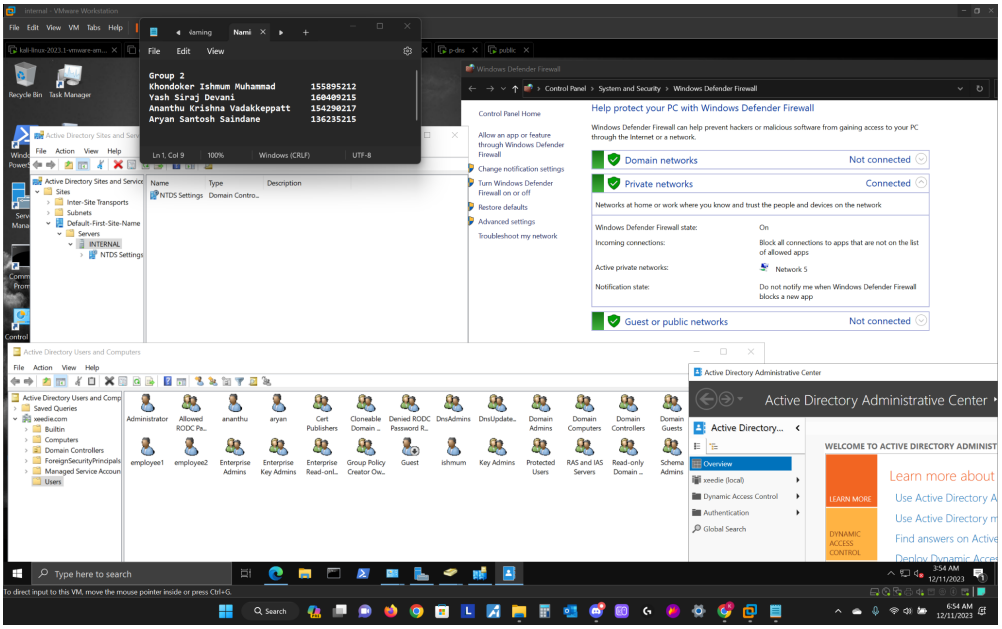


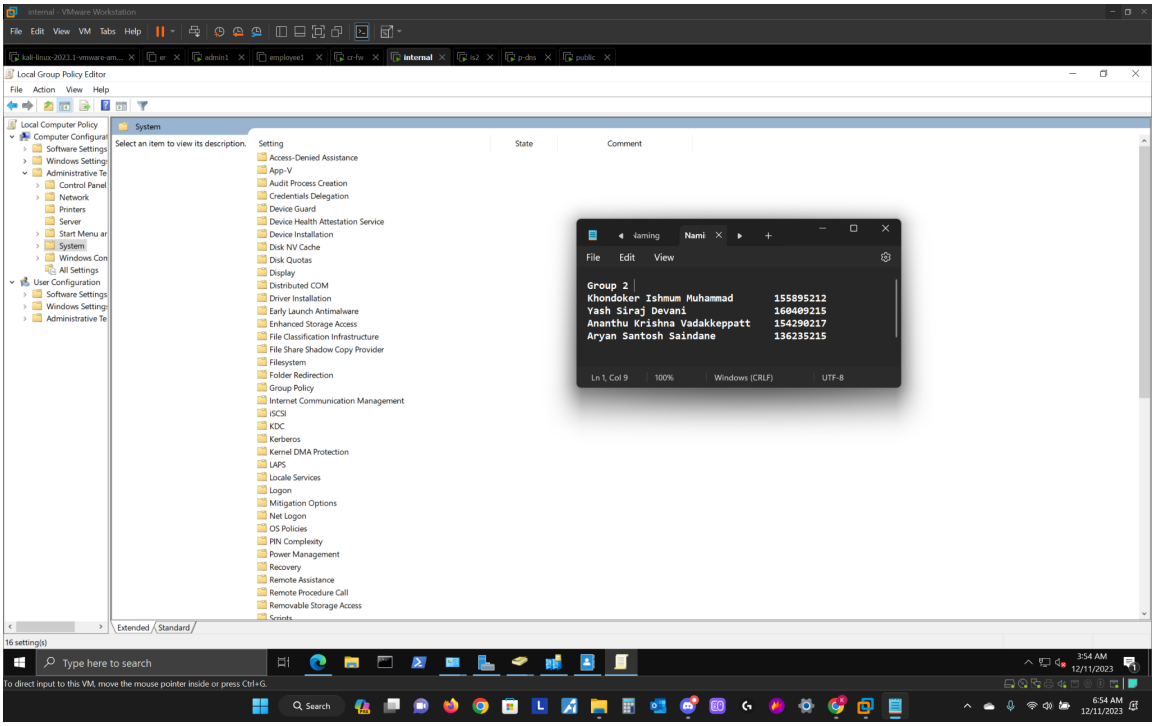
12. Incident Response Planning

- Stress the importance of creating an incident response plan to efficiently handle and mitigate the impact of phishing incidents. Incident response planning is a pivotal step in the field of cyber security. It can be used to handle and mitigate security breaches in a structured and well organized manner. The planning must utilize identifying potential threats, fast actions to come up with a plan to mitigate the threats so that the level of impact can be reduced.

13. Regular Security Assessments for Active Directory

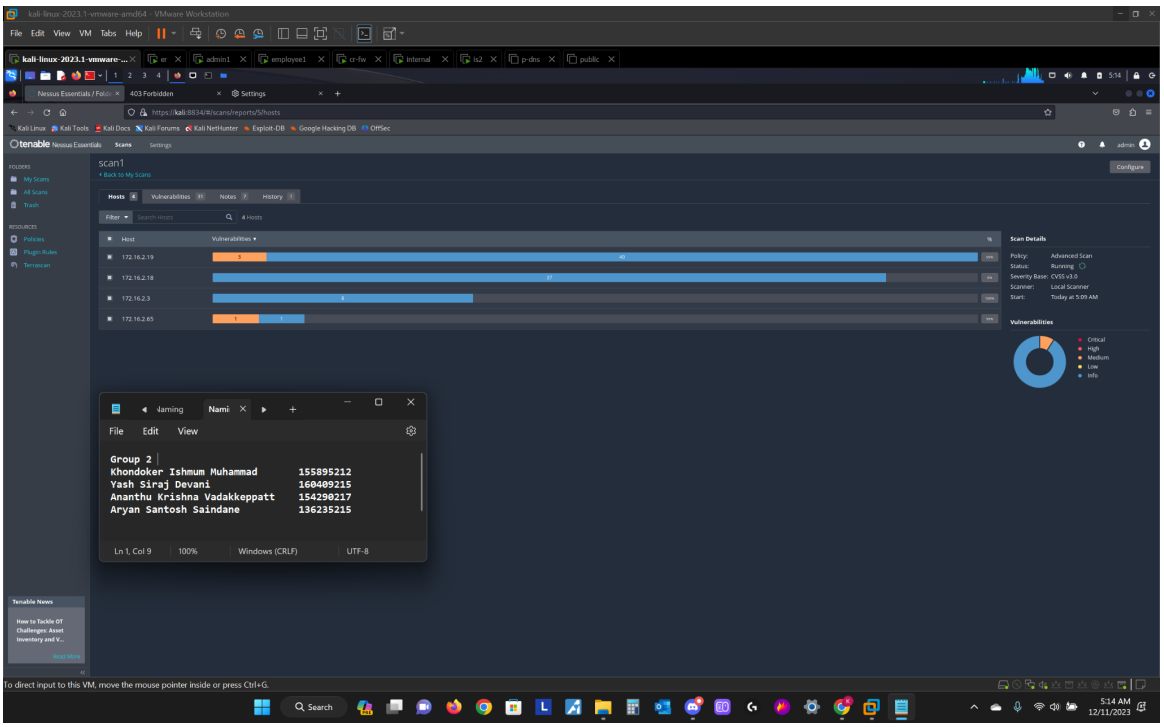
- Highlight the need for regular security assessments and penetration testing to identify and address vulnerabilities in the Active Directory environment. Also making sure to check active directory group policies.





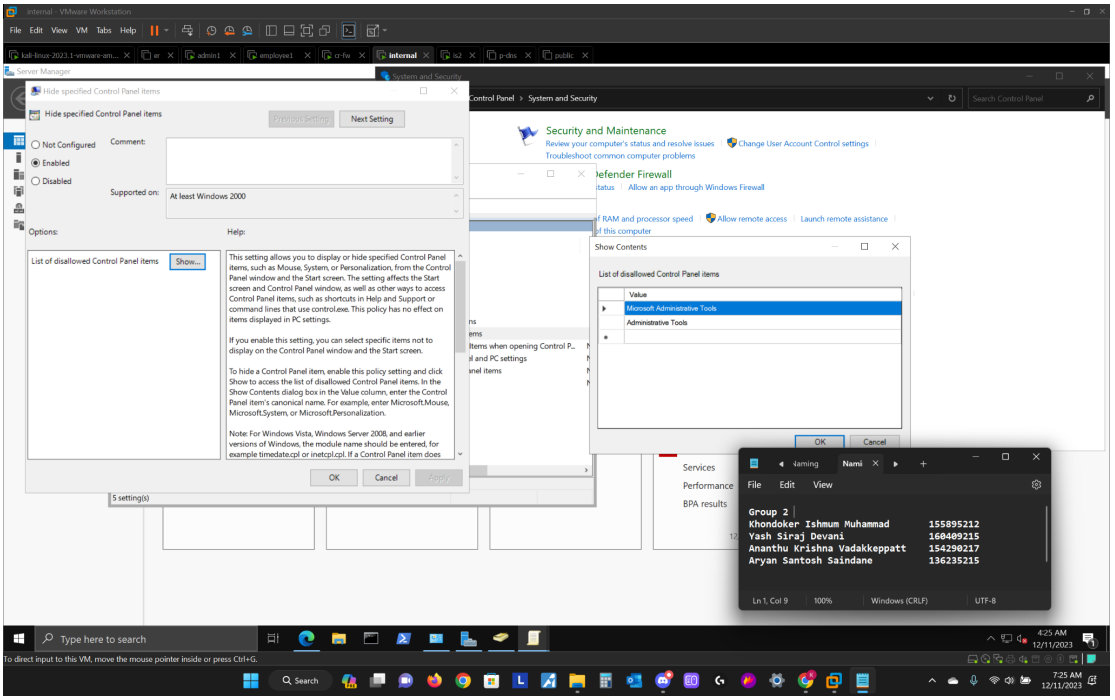
14. Lateral Movement Prevention

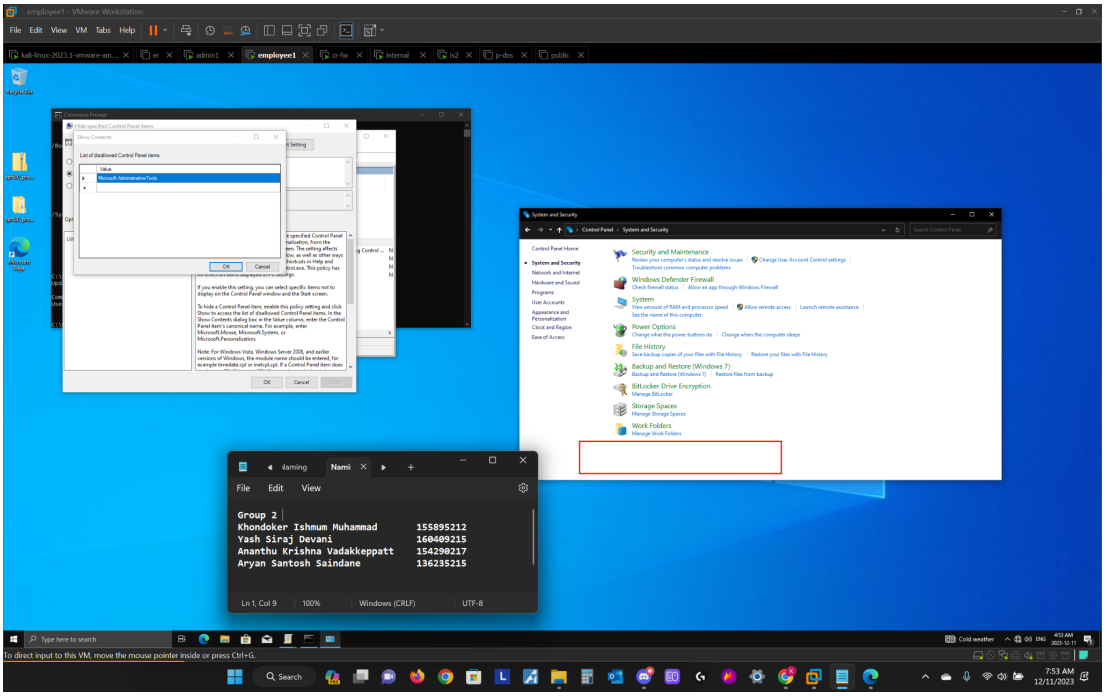
- Conduct regular penetration testing to identify and eliminate potential lateral movement paths. This can be done through scans to find out vulnerabilities and then seeing if those vulnerabilities can be exploited. ThenAfter exploiting those vulnerabilities, steps should be taken to patch those vulnerabilities to mitigate their risks. By patching these vulnerabilities we can prevent malicious actors from pivoting from one device to another. This in turn can also prevent malicious actors from Gaining unauthorized access to confidential data.



15. Account Access Management

- Ensuring robust access management is essential for enterprise security, incorporating measures like role-based access permissions so that users who are not authorized do not get access to unauthorized admin tools. As we can see below, administrative tools no longer appear for employee user.

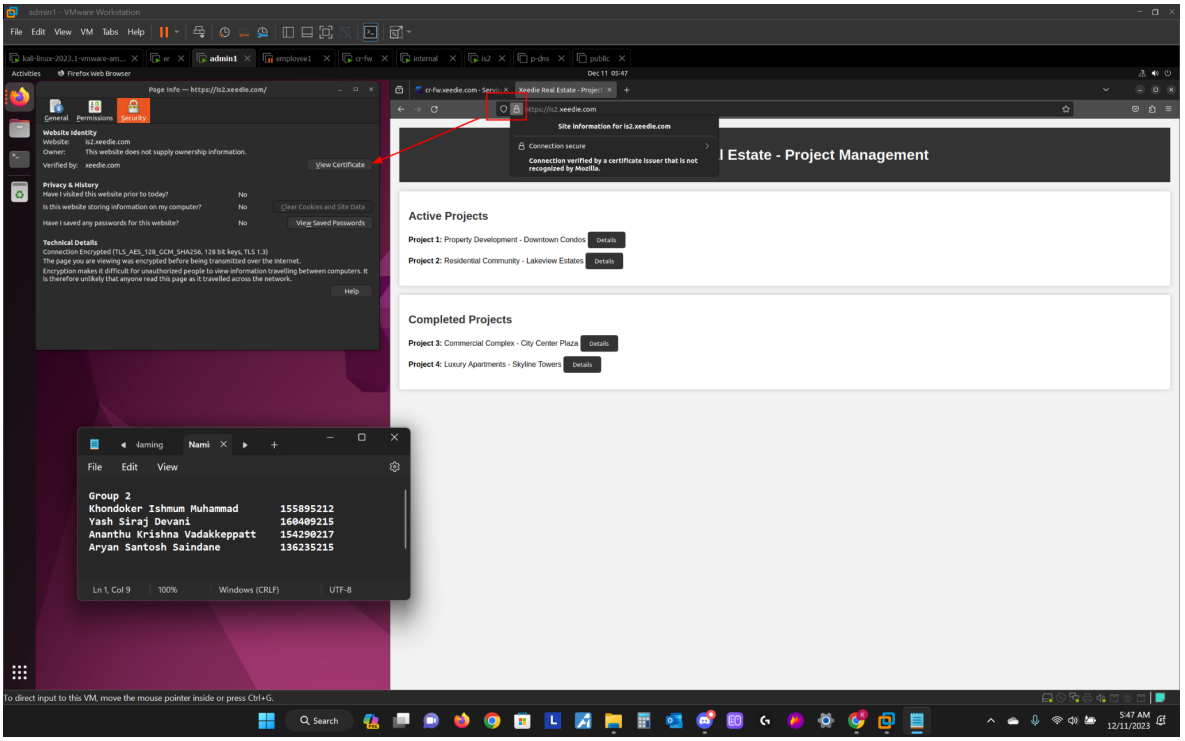


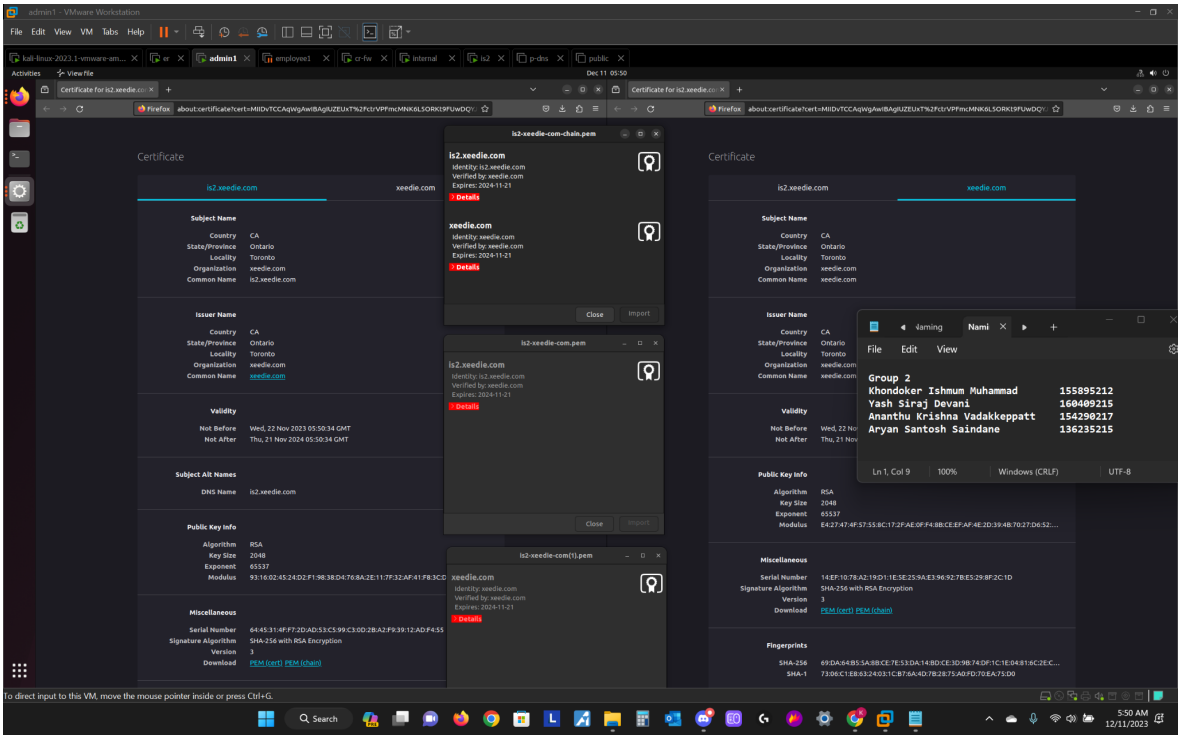


16. SSL Certificates & CA For Secure HTTPS and Trust In Browser.

- Implementing SSL certificates is pivotal for enhancing security, providing encrypted communication between users' browsers and servers to prevent unauthorized

access and safeguard sensitive information during data transmission. Also utilize SSL Certificate CA and create certificate chains to ensure trust in browsers.



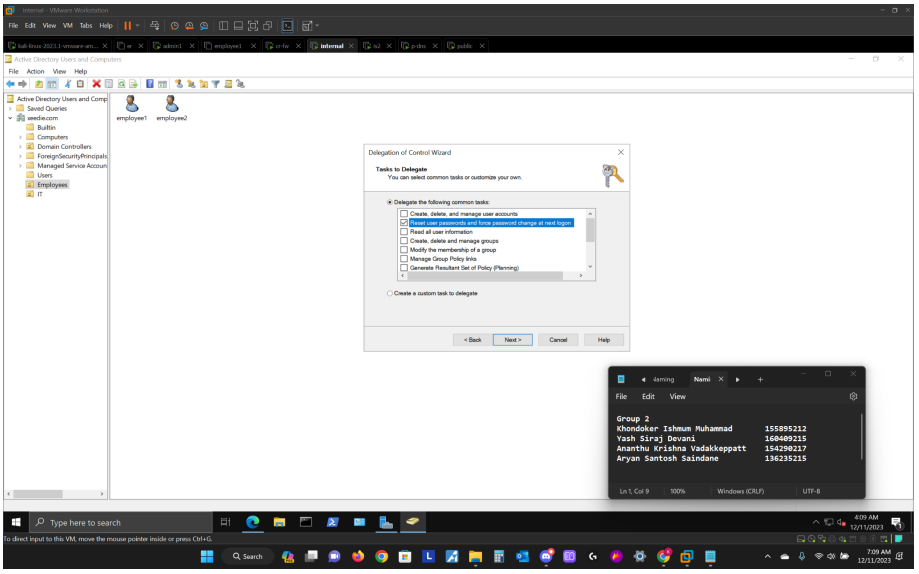


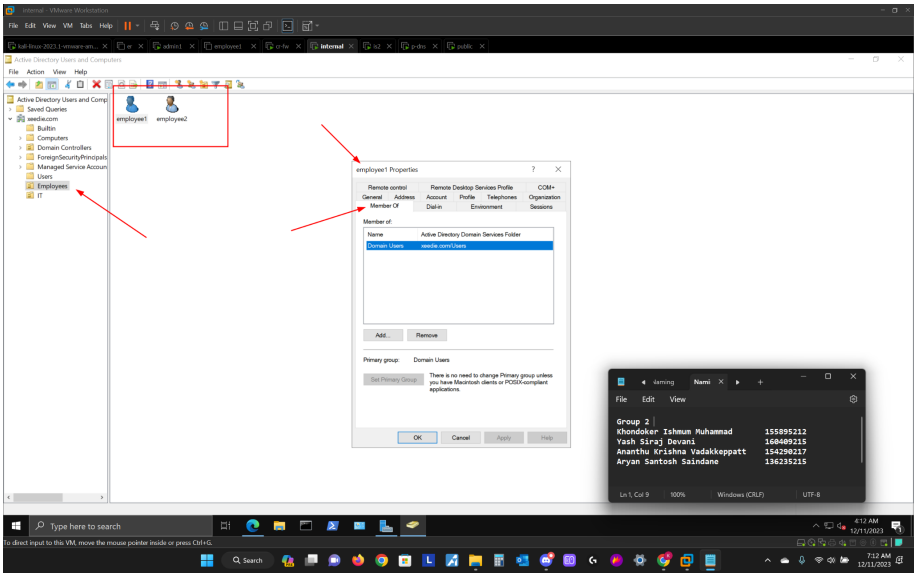
17. Host based Firewall utilization

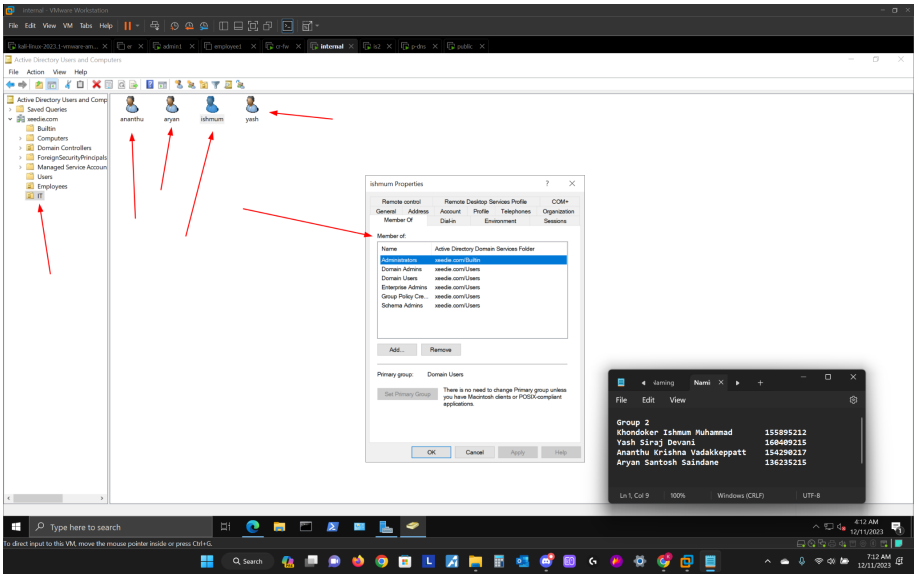
- Using a host-based firewall to proactively block malicious traffic, ensuring the security of the network.

18. Active Directory Domain User & Groups Management

- Ensuring robust user and group management is essential for enterprise security, incorporating measures like setting specific roles for specific users and adding users in groups depending on their title is essential for a secure environment and to mitigate the risk of unauthorized access to sensitive data.






Active Directory Users and Computers
ananthu
aryan
ishmum
yash
ishmum Properties
Member of:
Domain Users
Group 2
Khondoker Ishmum Muhammad 155895212
Yash Siraj Devani 168409215
Ananthu Krishna Vadakkeppatt 154298217
Aryan Santosh Saindane 136235215

Conclusion

The security testing report for Agricore's infrastructure signifies the successful integration of security controls in alignment with CIS recommendations. Notably, access management controls, including Role-Based Access Control (RBAC) facilitated by Group Policy Objects (GPOs), were implemented to assign authorized personnel appropriate access privileges. The report emphasizes the effective deployment of audit log management controls, utilizing Snort IDS to establish robust logging mechanisms for monitoring and responding to suspicious activities. Additional measures were taken to bolster web browser security through the implementation and testing of SSL. Furthermore, a thorough evaluation of data backup and recovery solutions ensured the reliability of backup processes. In conclusion, the report affirms the establishment of a well-designed security control framework within the Agricore infrastructure, demonstrating a proactive approach to fortifying defenses against potential threats and vulnerabilities.